On the ring of invariants of ordinary quartic curves in characteristic 2

Jürgen Müller and Christophe Ritzenthaler [1]

1 Introduction

Traditionally, non-singular curves of a fixed genus g are classified in two categories, those which are hyperelliptic and those which are not. The first ones are usually considered to be the simplest, since their geometry relies on their Weierstra points and is condensed on a line. Thus, the hyperelliptic locus $\mathcal{M}_g^h$ of the corresponding moduli space $\mathcal{M}_g$ is easily described and well understood. Seen from an invariant theoretical viewpoint, this is reflected by the fact that one only needs to deal with binary forms. To the contrary, non-hyperelliptic curves are more involved. Even in the simplest case, non-singular quartic curves over $\mathbb{C}$, no complete description of the relevant invariant ring is known. More precisely, for the invariant ring of the natural action of $SL_3(\mathbb{C})$ on the vector space of homogeneous polynomials of degree 4 in 3 variables a set of primary invariants, see [6], but no complete algebra generating set is known; a conjecture of Shioda says that the invariant ring is generated as an algebra by 13 elements.

Hence the question arises whether we can describe the situation more precisely over other fields? If F is a finite field of characteristic 2, in [10] a complete classification of the F-isomorphism types of non-singular quartic curves defined over F has been obtained. Moreover, the stratification of the non-hyperelliptic locus $\mathcal{M}_3^{nh}$ of the moduli space $\mathcal{M}_3$ with respect to the 2-rank of the Jacobian, and the F-rational points on the various strata, have been described there. Here, the generic case is the one of ordinary non-singular quartic curves, where the 2-rank of the Jacobian is maximal, hence equal to 3. In [10], a precise description of the ordinary non-singular quartic curves is given, and it is shown that the invariant ring associated to their moduli space $\mathcal{M}_3^{ord}$ is given by a linear action of the finite group $G = GL_3(\mathbb{F}_2)$ on a 6-dimensional vector space W'^*, being defined over the field $\mathbb{F}_2$ with 2 elements. The aim of the present note is to give a complete and precise description of this invariant ring, being denoted $S[W'^*]^G$ in the sequel, thereby answering the corresponding question posed in [10].

Despite the precise description of G and W'^*, being suitable to be handled by computer algebra systems, brute force computer calculations to find primary and secondary invariants of $S[W'^*]^G$, using the standard press-button algorithms implemented in MAGMA [4], as well as at most 2 Gigabytes of memory and several hours of computing time, had to be abandoned unsuccessfully. Hence the strategy employed here is to intertwine theoretical and computational analysis

[1] C. Ritzenthaler acknowledges financial support provided through the European Community's Human Potential Programme under contract HPRN-CT-2000-00114, GTEM.

of $S[W'^*]^G$, which in effect leads both to some structural understanding of $S[W'^*]^G$ and finally to explicitly given invariants. Actually, the theoretical analysis indicates how to combine ideas from computational invariant theory and tools already available in computer algebra systems to obtain specially tailored techniques applicable to the examples at hand. Finally, the necessary computations have been carried out the computer algebra systems MAGMA [4] and GAP [8]. After all, to check the correctness of the results only needs a few seconds of computing time and approximately 10 Megabytes of memory. More details of the computations, a MAGMA input file, as well as the primary and secondary invariants calculated, can be found on: `http://www.math.jussieu.fr/~ritzenth`.

More precisely, the ring $S[W'^*]^G$ turns out to be Cohen-Macaulay, an optimal set of primary invariants has degrees $\{2, 3, 3, 4, 6, 7\}$, and a corresponding minimal set of secondary invariants has cardinality 18. Moreover, the algebra $S[W'^*]^G$ is generated by at most $12 = 6+6$ invariants, namely the 6 primary invariants and 6 of the secondary invariants, the latter having degrees $\{0, 4, 5, 5, 6, 7\}$. Hence in particular $S[W'^*]^G$ is generated by invariants of degree at most 7. By the way, the number 12 rings a bell: The authors wonder whether there is a connection to Shioda's conjecture mentioned above.

The paper is organized as follows: In Section 2 we prepare the setting on ordinary quartic curves, recall the necessary facts from [10], and exhibit the G-module W'^* whose invariant ring $S[W'^*]^G$ we are going to examine. In Section 3 we recall a few notions from commutative algebra and derive some general facts about invariant rings needed in the sequel. Finally, in Section 4 we carry out the analysis of the invariant ring $S[W'^*]^G$. Note that we consider right group actions throughout, as this is common is the computer algebra community and assumed in the computer algebra systems used.

2 Ordinary quartic curves

(2.1) Let $\mathbb{F}_2$ be the finite field with 2 elements, and let $\overline{\mathbb{F}}_2$ be its algebraic closure. Let $M := \mathbb{F}_2^3$ be the 3-dimensional (row) vector space over $\mathbb{F}_2$, and let $\overline{M} := M \otimes_{\mathbb{F}_2} \overline{\mathbb{F}}_2$. Moreover, let $W := \mathbb{F}_2^7$ and $\overline{W} := W \otimes_{\mathbb{F}_2} \overline{\mathbb{F}}_2$, and let $\mathcal{C} := \{C_{a,b,c,d,e,f,g}; 0 \neq [a,b,c,d,e,f,g] \in \overline{W}\}$ be the family of quartic curves given by

$$C_{a,b,c,d,e,f,g} \colon Q^2_{a,b,c,d,e,f} = g^2 \cdot xyz(x+y+z),$$

where $Q_{a,b,c,d,e,f} := ax^2 + by^2 + cz^2 + dxy + eyz + fzx$. This family is important because of the following

(2.2) Proposition. See [10, Prop.1.1].
Let C be a non-singular quartic curve defined over $\overline{\mathbb{F}}_2$. Then the following conditions are equivalent:
i) The Jacobian variety J_C of C is ordinary, i. e. we have $|J_C[2](\overline{\mathbb{F}}_2)| = 2^3$.
ii) The curve C has seven bitangents.

iii) The curve C is isomorphic to some curve $C_{a,b,c,d,e,f,g} \in \mathcal{C}$ such that

$$(*) \qquad abcg(a+b+d)(b+c+e)(a+c+f)(a+b+c+d+e+f+g) \neq 0. \qquad \sharp$$

Moreover, non-singular quartic curves C and C' are isomorphic, if and only if there is an element $\gamma \in GL_3(\overline{\mathbb{F}}_2)$ such that $C^\gamma = C'$, where $\mathbb{P}(\overline{M})$ is considered as the natural right module for the projective general linear group $PGL_3(\overline{\mathbb{F}}_2)$ of rank 3 over $\overline{\mathbb{F}}_2$, and C^γ is the curve defined by

$$V(C^\gamma) := \{[x,y,z] \in \mathbb{P}(\overline{M}); [x,y,z] \cdot \gamma^{-1} \in V(C)\},$$

where $V(\cdot)$ denotes the locus of points of the curve. Using the action on the 7 bitangents, the isomorphism issue is reduced to the finite group $G := GL_3(\mathbb{F}_2) = PGL_3(\mathbb{F}_2) \leq PGL_3(\overline{\mathbb{F}}_2)$. Indeed, non-singular curves $C_{a,b,c,d,e,f,g} \in \mathcal{C}$ and $C_{a',b',c',d',e',f',g'} \in \mathcal{C}$ are isomorphic, if and only if there is an element $\gamma \in G$ such that $(C_{a,b,c,d,e,f,g})^\gamma = C_{a',b',c',d',e',f',g'}$, see [10].

(2.3) In the sequel let $G := GL_3(\mathbb{F}_2)$ be the general linear group of degree 3 over $\mathbb{F}_2$, which up to isomorphism is the unique simple group of order 168, see [3, p.3]. Let $A, B, C \in G$ be the elements of order 2, 3 and 7, respectively, defined as

$$A := \begin{bmatrix} 1 & . & 1 \\ . & 1 & . \\ . & . & 1 \end{bmatrix}, \quad B := \begin{bmatrix} . & . & 1 \\ 1 & . & . \\ . & 1 & . \end{bmatrix}, \quad C := \begin{bmatrix} . & 1 & . \\ . & . & 1 \\ 1 & 1 & . \end{bmatrix}.$$

It is easily checked using GAP or MAGMA that $G = \langle A, B \rangle$. The $\mathbb{F}_2$-vector space M can be considered as the natural right module for G. As the above action of $PGL_3(\overline{\mathbb{F}}_2)$ restricts to an action of G on $\mathcal{C}$, it is easily checked that we get an $\mathbb{F}_2$-linear action of G on W as

$$D_W\colon \quad A \mapsto \left[\begin{array}{ccc|ccc|c} 1 & . & . & . & . & . & . \\ . & 1 & . & . & . & . & . \\ 1 & . & 1 & . & . & . & . \\ \hline . & . & . & 1 & . & . & . \\ . & . & . & 1 & 1 & . & . \\ 1 & . & . & . & . & 1 & . \\ \hline . & . & . & 1 & . & . & 1 \end{array}\right], \quad B \mapsto \left[\begin{array}{ccc|ccc|c} . & . & 1 & . & . & . & . \\ 1 & . & . & . & . & . & . \\ . & 1 & . & . & . & . & . \\ \hline . & . & . & . & . & 1 & . \\ . & . & . & 1 & . & . & . \\ . & . & . & . & 1 & . & . \\ \hline . & . & . & . & . & . & 1 \end{array}\right].$$

The $\mathbb{F}_2$-subspace $W' := \{[a,b,c,d,e,f,g] \in W; g = 0\} \leq W$ is a G-submodule of W, and the above matrices show that $W/W' \cong \mathbb{F}_2$ is the trivial G-module. Hence we have an extension of G-modules

$$(**) \qquad \{0\} \to W' \to W \to \mathbb{F}_2 \to \{0\}.$$

Moreover, there is a G-submodule $W'' \leq W'$, such that $\dim_{\mathbb{F}_2}(W'') = 3$, as is also indicated above. The characteristic polynomials of the action of $C \in G$ on

W'' and W'/W'' are $t^3+t+1 \in \mathbb{F}_2[t]$ and $t^3+t^2+1 \in \mathbb{F}_2[t]$, respectively, which both are irreducible. Hence by [9, p.3] we conclude that W'' and W'/W'' are non-isomorphic absolutely irreducible G-modules, where $W'' \cong M$ is isomorphic to the natural representation of G, and W'/W'' is obtained from W'' by applying the automorphism of G given by inverting and transposing matrices.

(2.4) Let $\eta \in Z^1(G, W')$ be the cocycle describing the extension $(**)$, and let $\mathcal{S}_4 \cong H \leq G$ be the subgroup permuting the set $\{x^*, y^*, z^*, (x+y+z)^*\} \subseteq M^*$, where $M^* := \mathrm{Hom}_{\mathbb{F}_2}(M, \mathbb{F}_2)$ is the G-module contragredient to M and $\{x^*, y^*, z^*\} \subseteq M^*$ is the $\mathbb{F}_2$-basis dual to the standard basis of M.

By construction, for the restriction of η to the subgroup H we have $\eta|_H = 0 \in Z^1(H, W')$. As $[G\colon H] = 7$ is invertible in $\mathbb{F}_2$, we by [1, Cor.3.6.18] conclude that $\eta = 0 \in H^1(G, W') \cong \mathrm{Ext}^1_G(\mathbb{F}_2, W')$. Thus the extension $(**)$ splits, and we have $W = W' \oplus \mathbb{F}_2$ as G-modules. More concretely, going over from the standard basis of W to the $\mathbb{F}_2$-basis where the last standard basis vector is replaced by $[1,1,1,1,1,1,1] \in W$, we indeed obtain

$$D'_W\colon \quad A \mapsto \left[\begin{array}{ccc|ccc|c} 1 & . & . & . & . & . & . \\ . & 1 & . & . & . & . & . \\ 1 & . & 1 & . & . & . & . \\ \hline . & . & . & 1 & . & . & . \\ . & . & . & 1 & 1 & . & . \\ 1 & . & . & . & . & 1 & . \\ \hline . & . & . & . & . & . & 1 \end{array}\right], \quad B \mapsto \left[\begin{array}{ccc|ccc|c} . & . & 1 & . & . & . & . \\ 1 & . & . & . & . & . & . \\ . & 1 & . & . & . & . & . \\ \hline . & . & . & . & . & 1 & . \\ . & . & . & 1 & . & . & . \\ . & . & . & . & 1 & . & . \\ \hline . & . & . & . & . & . & 1 \end{array}\right].$$

Actually, this basis change amounts to substituting the curves $C_{a,b,c,d,e,f,g} \in \mathcal{C}$ by curves defined by

$$(ax^2 + by^2 + cz^2 + dxy + eyz + fzx)^2 = g^2 \cdot C_K(x,y,z),$$

where $C_K(x,y,z) = x^4+y^4+z^4+(xy)^2+(yz)^2+(zx)^2+xyz(x+y+z)$. We have $x^{*4}+y^{*4}+z^{*4}+(x^*y^*)^2+(y^*z^*)^2+(z^*x^*)^2+x^*y^*z^*(x^*+y^*+z^*) \in S[M^*]^G$ by construction, where $S[M^*]^G \subseteq S[M^*]$ denotes the $\mathbb{F}_2$-subalgebra of G-invariants of the symmetric algebra $S[M^*]$ over M^*. As for the homogeneous component $S[M^*]^G_4$ of $S[M^*]^G$ of degree 4 we have $\dim_{\mathbb{F}_2}(S[M^*]^G_4) = 1$, see [7], the curve $C_K \subseteq \mathbb{P}(\overline{M})$ is a twist of the Klein quartic curve.

As the extension $(**)$ splits, for the corresponding contragredient G-modules we have $W^* \cong W'^* \oplus \mathbb{F}_2^*$. With respect to the $\mathbb{F}_2$-basis $\{a^*, b^*, c^*, d^*, e^*, f^*\} \subseteq W'^*$ dual to the standard basis of W', the G-action on W'^* is given as

$$D_{W'^*}\colon \quad A \mapsto \left[\begin{array}{ccc|ccc} 1 & . & 1 & . & . & 1 \\ . & 1 & . & . & . & . \\ . & . & 1 & . & . & . \\ \hline . & . & . & 1 & 1 & . \\ . & . & . & . & 1 & . \\ . & . & . & . & . & 1 \end{array}\right], \quad B \mapsto \left[\begin{array}{ccc|ccc} . & . & 1 & . & . & . \\ 1 & . & . & . & . & . \\ . & 1 & . & . & . & . \\ \hline . & . & . & . & . & 1 \\ . & . & . & 1 & . & . \\ . & . & . & . & 1 & . \end{array}\right].$$

Let $\overline{W'^*} := W'^* \otimes_{\mathbb{F}_2} \overline{\mathbb{F}}_2$ and $\overline{W'} := W' \otimes_{\mathbb{F}_2} \overline{\mathbb{F}}_2$. Moreover, let $S[W'^*]$ denote the symmetric $\mathbb{F}_2$-algebra over W'^*. Hence we have $S[\overline{W'^*}] \cong S[W'^*] \otimes_{\mathbb{F}_2} \overline{\mathbb{F}}_2$. Moreover, by Remark (3.5) below we have $S[\overline{W'^*}]^G \cong S[W'^*]^G \otimes_{\mathbb{F}_2} \overline{\mathbb{F}}_2$. The embedding of affine rings $S[\overline{W'^*}]^G \subseteq S[\overline{W'^*}]$, where $S[\overline{W'^*}]^G$ is the ring of G-invariants in $S[\overline{W'^*}]$, defines a morphism $\overline{W'} \to \overline{W'}/G$ of affine varieties over $\overline{\mathbb{F}}_2$, which as G is finite is a geometric quotient, see [5, Ch.2.3]. Hence we have proved the following

(2.5) Proposition. See [10, Prop.1.3].
The moduli space $\mathcal{M}_3^{ord}$ of the ordinary quartic curves is isomorphic to the open subset of the affine variety $\mathrm{Spec}(S[W'^*]^G \otimes_{\mathbb{F}_2} \overline{\mathbb{F}}_2)$ given by the non-singularity conditions $(*)$, see Proposition (2.2). $\sharp$

3 Invariant rings

We recall a few notions from commutative algebra and derive some general facts about invariant rings; as general references see e. g. [2, 5]. Note that we use the following piece of notation frequently: If $\mathcal{E}$ is a subset of a commutative ring R, then $\mathcal{E}R$ denotes the ideal of R generated by $\mathcal{E}$.

(3.1) Definition. Let $R = \bigoplus_{d \geq 0} R_d$ be a finitely generated commutative $\mathbb{Z}^{\geq 0}$-graded algebra over a field F, such that $\dim_F(R_d) < \infty$ for $d \in \mathbb{N}_0$, and $R_0 \cong F$. Let $R_+ := \bigoplus_{d>0} R_d \triangleleft R$ be the **irrelevant ideal**, and let $H_R(t) \in \mathbb{Q}(t) \subseteq \mathbb{Q}((t))$ denote the **Hilbert series** of R.

A set $\mathcal{F} := \{f_1, \ldots, f_n\} \subseteq R_+$ of homogeneous elements, where $n = \dim(R)$ is the **Krull dimension** of R, is called a **homogeneous system of parameters**, if $\mathcal{F}$ is algebraically independent and if R is a finitely generated $F[\mathcal{F}]$-module, where $F[\mathcal{F}] \subseteq R$ is the polynomial F-subalgebra of R generated by $\mathcal{F}$.

(3.2) Definition. The F-algebra R is called **Cohen-Macaulay** if there is a homogeneous system of parameters $\mathcal{F}$ such that R is a free $F[\mathcal{F}]$-module. If R is Cohen-Macaulay, then R is a free $F[\mathcal{F}]$-module for each homogeneous system of parameters $\mathcal{F}$. Moreover, R is Cohen-Macaulay if and only if $\dim(R) = \mathrm{depth}(R)$. Here the **depth** of R is the common length of all maximal **regular** homogeneous sequences in R, see [2, Ch.4.3]. Note that each regular sequence can be extended to a maximal one; and if R is Cohen-Macaulay, then the homogeneous systems of parameters of R and the maximal regular homogeneous sequences in R coincide.

(3.3) Remark. Let R be Cohen-Macaulay, and let $\mathcal{F} = \{f_1, \ldots, f_n\} \subseteq R$ be a homogeneous system of parameters. Hence R is a free $F[\mathcal{F}]$-module, and for a minimal homogeneous $\mathcal{F}$-module generating set $\mathcal{G} = \{g_1, \ldots, g_s\}$ of R we have

$$H_R(t) = \frac{\sum_{j=1}^{s} t^{e_j}}{\prod_{i=1}^{n}(1 - t^{d_i})} \in \mathbb{Q}(t),$$

where $d_i = \deg(f_i)$ and $e_j = \deg(g_j)$. Hence in the Cohen-Macaulay case the degrees d_i and e_j of the elements of $\mathcal{F}$ and $\mathcal{G}$ can be read off from H_R.

(3.4) Definition. Let G be a finite group, let V be an FG-module and let $S[V]^G$ denote the ring of **G-invariants** in the symmetric algebra $S[V]$ over V. By [2, Thm.1.3.1] the F-algebra $S[V]^G$ is finitely generated and we have $\dim(S[V]^G) = \dim(S[V]) = \dim_F(V)$. A homogeneous system of parameters $\mathcal{F}$ of $S[V]^G$ is called a set of **primary invariants**. A minimal set of homogeneous $F[\mathcal{F}]$-module generators of R is called a set of **secondary invariants**.

(3.5) Remark. Let $F \subseteq L$ be a field extension, and let $V_L := V \otimes_F L$. As for $d \in \mathbb{N}_0$ we have $S[V]_d^G = \bigcap_{\sigma \in G} \ker_{S[V]_d}(\sigma - 1)$, we conclude that $\dim_F(S[V]_d^G) = \dim_L(S[V_L]_d^G)$, for $d \in \mathbb{N}_0$. Thus we have $S[V]^G \otimes_F L = S[V_L]^G$.

(3.6) Definition. Let $H \leq G$ be a subgroup such that the characteristic $\mathrm{char}(F)$ of the field F does not divide the index $[G \colon H]$ of H in G. Then the **relative Reynolds operator** with respect to H and G is defined as

$$\mathcal{R}_H^G \colon S[V]^H \to S[V]^G \colon f \mapsto \frac{1}{[G \colon H]} \cdot \sum_{\sigma \in H|G} f \cdot \sigma,$$

where the sum runs over a set of representatives of the right cosets $H|G$ of H in G. Note that we have $S[V]^G \subseteq S[V]^H$, and hence $\mathcal{R}_H^G$ is an $S[V]^G$-module projection onto $S[V]^G$.

The following Proposition is a slight generalization of the Hochster-Eagon Theorem, see [2, Thm.4.3.6], saying that if $\mathrm{char}(F)$ does not divide $|G|$, then $S[V]^G$ is Cohen-Macaulay; see also [11, Prop.8.3.1].

(3.7) Proposition. Let $H \leq G$ be a subgroup such that $\mathrm{char}(F)$ does not divide $[G \colon H]$. Provided $S[V]^H$ is Cohen-Macaulay, then $S[V]^G$ is Cohen-Macaulay as well.

Proof. Let $\mathcal{F} \subseteq S[V]^G$ be a set of primary invariants of $S[V]^G$. As both $F[\mathcal{F}] \subseteq S[V]^G$ and $S[V]^G \subseteq S[V]^H$ are finite ring extensions, this also holds for $F[\mathcal{F}] \subseteq S[V]^H$, and hence $\mathcal{F} \subseteq S[V]^H$ is a set of primary invariants of $S[V]^H$. As $S[V]^H$ is Cohen-Macaulay, it hence is a free $F[\mathcal{F}]$-module. Using the relative Reynolds operator $\mathcal{R}_H^G$, we conclude that $S[V]^G$ is a direct summand of the graded $F[\mathcal{F}]$-module $S[V]^H$. Hence $S[V]^G$ is a finitely generated graded projective $F[\mathcal{F}]$-module, and thus by [2, La.4.1.1] is a free $F[\mathcal{F}]$-module. $\sharp$

(3.8) Remark. To compute primary invariants in our particular situation in Section 4, we will exploit the following setting.

Let $\{0\} \to U' \xrightarrow{\alpha} U \xrightarrow{\beta} V \to \{0\}$ be an extension of G-modules. Hence α induces an embedding $S[U'] \subseteq S[U]$, and β induces an isomorphism $S[U]/U'S[U] \to$

$S[V]$. Hence we have $S[U']^G \subseteq S[U]^G$ and $(S[U]/U'S[U])^G \cong S[V]^G$, where $U'S[U] \lhd S[U]$ is a G-submodule. Unfortunately, in general we only have an embedding $S[U]^G/(U'S[U])^G \subseteq (S[U]/U'S[U])^G$, but not an isomorphism, and in general $(U'S[U])^G \lhd S[U]^G$ is not generated by $S[U']^G_+$.

Let us assume that the above extension splits, and let $\gamma\colon V \to U$ such that $\gamma\beta = \mathrm{id}_V$. Hence γ induces an embedding $S[V] \subseteq S[U]$, and we have $S[U] = S[V] \oplus U'S[U]$ as G-modules. Thus from $S[U]^G = S[V]^G \oplus (U'S[U])^G$ we conclude that β induces an isomorphism $S[U]^G/(U'S[U])^G \cong S[V]^G$.

Let us moreover assume that $U' \cong F$ is the trivial G-module, and let $0 \neq \hat{f} \in U' \subseteq S[U]^G_1$. Then we have $(U'S[U])^G = \hat{f} \cdot S[U]^G \lhd S[U]^G$, and thus β induces an isomorphism $S[U]^G/\hat{f}S[U]^G \cong S[V]^G$. As $\hat{f} \in S[U]$ is not a zero-divisor, for the corresponding Hilbert series we obtain $H_{S[V]^G}(t) = (1-t)\cdot H_{S[U]^G}(t) \in \mathbb{Q}(t)$.

Let $\hat{\mathcal{F}} := \{\hat{f}_0, \ldots, \hat{f}_{n-1}\} \subseteq S[U]^G$ be a set of primary invariants, such that $\hat{f}_0 = \hat{f}$, and let $f_i := \hat{f}_i\beta \in S[V]^G$, for $i \in \{1, \ldots, n-1\}$, as well as $\mathcal{F} := \{f_1, \ldots, f_{n-1}\}$. Note that we have $n = \dim(S[U]^G) = \dim_F(U)$ and $n-1 = \dim(S[V]^G) = \dim_F(V)$. As $\hat{\mathcal{F}} \subseteq S[U]^G$ is a set of primary invariants, by the Graded Nakayama Lemma, see [5, La.3.5.1], we have $\dim(S[U]^G/\hat{\mathcal{F}}S[U]^G) = 0$. Hence using β we find $\dim(S[V]^G/\mathcal{F}S[V]^G) = 0$, where $|\mathcal{F}| \leq n-1$. Hence by the Graded Nakayama Lemma again we conclude that $\mathcal{F} \subseteq S[V]^G$ is set of primary invariants.

Finally, we note the following. As $\hat{f} \in S[U]^G$ is not a zero-divisor, and hence regular, we conclude that $S[U]^G$ is Cohen-Macaulay, if and only if $S[V]^G$ is. Moreover, if $S[V]^G$ is Cohen-Macaulay, then there is a maximal regular homogeneous sequence in $S[U]^G$ beginning with $\hat{f}$, which thus is a set of primary invariants of $S[U]^G$, and the above construction indeed yields a a set of primary invariants of $S[V]^G$, which is optimal in the sense of [5, Ch.3.3.2] if the used set of primary invariants of $S[U]^G$ was.

(3.9) Remark. To compute secondary invariants in our particular situation in Section 4, we use a special adaptation of the method typically used in the case where $\mathrm{char}(F)$ does not divide $|G|$, see [5, Ch.3.5].

Let us assume that $R := S[V]^G$ is known to be Cohen-Macaulay, and that the Hilbert series $H_R \in \mathbb{Q}(t)$ and a set $\mathcal{F} \subseteq R_+$ of primary invariants are known. Hence by Remark (3.3) we have $f := \prod_{i=1}^n (1-t^{d_i}) \cdot H_R \in \mathbb{Z}^{\geq 0}[t]$, and hence the cardinality s of any minimal homogeneous $F[\mathcal{F}]$-module generating set $\mathcal{G}$ of R is given as $s = f(1)$, while the degrees e_j can be determined from the monomials occurring in f.

Let $\mathcal{G} \subseteq R$ be a set having the appropriate cardinality, whose elements are homogeneous of the appropriate degrees. By the Graded Nakayama Lemma, see [5, La.3.5.1], the set $\mathcal{G}$ generates the $F[\mathcal{F}]$-module R, if and only if $\mathcal{G}$ generates the F-vector space $R/F[\mathcal{F}]_+R$. By the assumptions made on $\mathcal{G}$ we conclude that $\mathcal{G}$ is a generating set of the $F[\mathcal{F}]$-module R, if and only if $\mathcal{G} \subseteq R/F[\mathcal{F}]_+R$

is F-linearly independent.

As we are developing a method to find secondary invariants, the ring R and hence $R/F[\mathcal{F}]_+R$ are not yet known. Thus we proceed as follows. Let $H \leq G$ be a subgroup such that $\mathrm{char}(F)$ does not divide $[G\colon H]$, and let $S := S[V]^H$. As we have $F[\mathcal{F}] \subseteq R \subseteq S$, we may consider the natural map $\pi\colon R \to S \to S/(\sum_{i=1}^n f_iS)$ of F-algebras. Hence we have $F[\mathcal{F}]_+R \subseteq \ker(\pi)$. Conversely, let $h \in \ker(\pi) \trianglelefteq R$, hence we have $h = \sum_{i=1}^n f_ih_i$, where $h_i \in S$. Thus we have $h = \mathcal{R}_H^G(h) = \sum_{i=1}^n f_i \cdot \mathcal{R}_H^G(h_i) \in F[\mathcal{F}]_+R$, and hence $\ker(\pi) = F[\mathcal{F}]_+R$. Thus we have an embedding $\pi\colon R/F[\mathcal{F}]_+R \to S/(\sum_{i=1}^n f_iS)$. Hence $\mathcal{G} \subseteq R/F[\mathcal{F}]_+R$ is F-linearly independent, if and only if $\pi(\mathcal{G}) \subseteq S/(\sum_{i=1}^n f_iS)$ is.

Let us finally assume that $S = S[V]^H$ is Cohen-Macaulay, and that $\mathcal{G}' \subseteq S$ is a minimal set of secondary invariants; note that $\mathcal{F} \subseteq S$ is a set of primary invariants. As S is the free $F[\mathcal{F}]$-module generated by $\mathcal{G}'$, a description of S as a finitely presented commutative F-algebra can be derived using linear algebra techniques, see [5, Ch.3.6]. From that, a description of $S/(\sum_{i=1}^n f_iS)$ as a finitely presented commutative F-algebra is immediately derived. Hence the F-linear independence of $\pi(\mathcal{G}) \subseteq S/(\sum_{i=1}^n f_iS)$ is easily verified or falsified using Grbner basis techniques, see [5, Ch.3.5]. $\sharp$

4 The invariant ring $S[W'^*]^G$

Let again $G := GL_3(\mathbb{F}_2)$ and let $S[W'^*]^G$ be the invariant ring introduced in Section (2.4). We are prepared to analyze its structure, and begin with a module theoretic property of the G-module W.

(4.1) Proposition. The G-module W is a transitive permutation module.

Proof. If W were a transitive permutation module, the corresponding point stabilizer would be a subgroup of order 24, leading to the following sensible guess. As in Section (2.4), let $\mathcal{S}_4 \cong H \leq G$ be the subgroup permuting the set $\{x^*, y^*, z^*, (x+y+z)^*\} \subseteq M^*$. Hence H fixes $w_0 = [0,0,0,0,0,0,1] \in W$, and we are led to conjecture that $H = \mathrm{Stab}_G(w_0)$ and that $w_0 \cdot G \subseteq W$ is an $\mathbb{F}_2$-basis of W being permuted by G. To check this, let $C \in G$ be as in Section (2.3). Its action on W is given as

$$D_W\colon \quad C \mapsto \left[\begin{array}{ccc|ccc|c} . & . & 1 & . & . & . & . \\ 1 & . & 1 & . & . & . & . \\ . & 1 & . & . & . & . & . \\ \hline . & . & 1 & . & . & 1 & . \\ . & . & . & 1 & 1 & . & . \\ . & . & . & . & 1 & . & . \\ \hline . & . & . & . & 1 & . & 1 \end{array}\right].$$

Hence $\{C^i \in G; i = 0, \ldots, 6\} \subseteq G$ is a set of representatives of the right cosets $H|G$, and $\Omega := \{w_0 \cdot C^i \in W; i = 0,6,1,2,3,4,5\} \subseteq W$ is given as follows, where

the rows indicate the elements of Ω in terms of the standard basis of W,

$$\begin{bmatrix} . & . & . & . & . & . & 1 \\ . & . & . & . & . & 1 & 1 \\ . & . & . & . & 1 & . & 1 \\ . & . & . & 1 & . & . & 1 \\ . & . & 1 & . & 1 & 1 & 1 \\ . & 1 & . & 1 & 1 & . & 1 \\ 1 & . & . & 1 & . & 1 & 1 \end{bmatrix}.$$

Hence Ω is an $\mathbb{F}_2$-basis of W, and it is easily checked that it is permuted by G, where in particular $A \mapsto (1,4)(2,7) \in \mathcal{S}_7$ and $B \mapsto (2,4,3)(5,7,6) \in \mathcal{S}_7$. $\sharp$

By Proposition (4.1) the G-module W'^* is a direct summand of the permutation module W^*. Note that direct summands of permutation modules are also called **trivial source modules**, see [5, Ch.3.10.4].

(4.2) Proposition. The Hilbert series $H_{S[W'^*]^G} \in \mathbb{Q}(t)$ of $S[W'^*]^G$ is given as

$$H_{S[W'^*]^G}(t) = \frac{1+t^4+2t^5+t^6+t^7+t^8+2t^9+2t^{10}+t^{11}+t^{12}+t^{13}+2t^{14}+t^{15}+t^{19}}{(1-t^2)\cdot(1-t^3)^2\cdot(1-t^4)\cdot(1-t^6)\cdot(1-t^7)}.$$

Proof. As the G-module W'^* is a trivial source module, by [1, Cor.3.11.4] the G-module W'^* has a unique lift to a trivial source $\mathbb{Z}_2G$-module $\widehat{W'^*}$, where $\mathbb{Z}_2 \subseteq \mathbb{Q}_2$ is the integral closure of $\mathbb{Z}$ in the 2-adic completion $\mathbb{Q}_2$ of $\mathbb{Q}$. Let $\widetilde{W'^*} := \widehat{W'^*} \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$. By [5, Prop.3.10.15] we have $H_{S[W'^*]^G}(t) = H_{S[\widetilde{W'^*}]^G}(t) \in \mathbb{Q}(t)$, where by Molien's Theorem, see [2, Thm.2.5.2], the latter is given as

$$H_{S[\widetilde{W'^*}]^G}(t) = \frac{1}{|G|} \cdot \sum_{\sigma \in G} \frac{1}{\det_{\widetilde{W'^*}}(1-t\sigma)} \in \mathbb{Q}_2(t).$$

Moreover, we have $\det_{\widetilde{W'^*}}(1-t\sigma) = \prod_{i=1}^{7}(1-\lambda_i(\sigma)\cdot t)$, where $\{\lambda_1(\sigma), \ldots, \lambda_7(\sigma)\}$ are the eigenvalues of the action of $\sigma \in G$ in a suitable extension field of $\mathbb{Q}_2$. Hence $\det_{\widetilde{W'^*}}(1-t\sigma)$ can be evaluated from the ordinary character table of G, see [3, p.3], and the character $\chi_{\widetilde{W'^*}}$ of $\widetilde{W'^*}$, see [2, Ch.2.5]. This method is implemented in GAP, where also the ordinary character table of G is available.

Hence it remains to find the character $\chi_{\widetilde{W'^*}}$. Thus we have to determine the trivial source lift $\widehat{W'^*}$. By the proof of Proposition (4.1) we have $(\mathbb{F}_2)_H^G \cong W \cong W' \oplus \mathbb{F}_2$, where $\mathbb{F}_2$ denotes the trivial G-module. Hence we have the trivial source lifts $(\mathbb{Z}_2)_H^G \cong \widehat{W} \cong \widehat{W'} \oplus \mathbb{Z}_2$, where again $\mathbb{Z}_2$ denotes the trivial G-module. Since we have $(\widehat{W})^* \cong \widehat{W^*}$ as G-modules, we obtain $((\mathbb{Z}_2)_H^G)^* \cong \widehat{W^*} \cong \widehat{W'^*} \oplus \mathbb{Z}_2$, Moreover, we conclude $((\mathbb{Q}_2)_H^G)^* \cong \widehat{W^*} \otimes_{\mathbb{Z}_2} \mathbb{Q}_2 \cong \widetilde{W'^*} \oplus \mathbb{Q}_2$. By [3, p.3] the character 1_H^G of the permutation G-module $(\mathbb{Q}_2)_H^G$ is given as $1_G + \chi_6$, where χ_6 is the unique irreducible character of degree 6 and 1_G is the trivial character. As χ_6 is real-valued, we hence have $\chi_{\widetilde{W'^*}} = 1_H^G - 1_G = \chi_6$. $\sharp$

(4.3) Proposition. The invariant ring $S[W'^*]^G$ is Cohen-Macaulay.

Proof. Let $D \leq G$ be a 2-Sylow subgroup of G, hence we have $|D| = 8$. Using the standard methods to compute primary invariants, see [5, Ch.3.3], and secondary invariants in the modular case, see [5, Ch.3.5], implemented in MAGMA, we find primary invariants $\{f'_1, \ldots, f'_6\} \subseteq S[W'^*]^D$ having degrees $\{1,1,2,2,2,4\}$, and a minimal set of secondary invariants $\mathcal{G}' := \{g'_0, \ldots, g'_3\} \subseteq S[W'^*]^D$ having degrees $\{0,3,3,6\}$, where of course $g'_0 = 1$. As we moreover have $|\mathcal{G}'| \cdot |D| = \prod_{i=1}^{6} \deg(f'_i)$, by [5, Thm.3.7.1] we conclude that $S[W'^*]^D$ is Cohen-Macaulay, and thus by Proposition (3.7) the ring $S[W'^*]^G$ also is. $\sharp$

(4.4) We are prepared to compute primary invariants of $S[W'^*]^G$. To do this, we first consider the permutation module $W^* = W'^* \oplus \mathbb{F}_2$, and compute the homogeneous components $S[W^*]^G_d$, for $d \leq 7$, as follows. Let $\Omega^* = \{\omega^*_1, \ldots, \omega^*_7\} \subseteq W^*$ be the $\mathbb{F}_2$-basis of W^* dual to the $\mathbb{F}_2$-basis $\Omega \subseteq W$ given in the proof of Proposition (4.1). As $S[W^*]_d$ also is a permutation module, whose $\mathbb{F}_2$-basis $(\Omega^*)^d$, consisting of the monomials of degree d in the indeterminates Ω^*, is permuted by G. Hence $(\Omega^*)^d$ is partitioned into G-orbits $(\Omega^*)^d = \coprod_{i=1}^{n_d} \mathcal{O}_i$, where $n_d = \dim_{\mathbb{F}_2}(S[W^*]^G_d)$. Letting $\mathcal{O}_i^+ := \sum_{f \in \mathcal{O}_i} f \in S[W^*]^G_d$ denote the corresponding orbit sum, the set $\{\mathcal{O}_i^+; i \in \{1, \ldots, n_d\}\}$ forms an $\mathbb{F}_2$-basis of $S[W^*]^G_d$, see also [5, Ch.3.10].

As by Remark (3.8) we have $H_{S[W^*]^G} = \frac{1}{1-t} \cdot H_{S[W'^*]^G} \in \mathbb{Q}(t)$, we look for primary invariants having degrees $\{1,2,3,3,4,6,7\}$. By [5, Prop.3.3.1], a set $\hat{\mathcal{F}} = \{\hat{f}_0, \ldots, \hat{f}_6\} \subseteq S[W^*]^G$ of homogeneous elements is a set of primary invariants, if and only if $\dim(S[W^*]/\hat{\mathcal{F}}S[W^*]) = 0$. Krull dimensions can be computed using Grbner basis techniques, which are implemented in MAGMA, and we indeed find the following set $\hat{\mathcal{F}}$ of primary invariants of $S[W^*]^G$, consisting of certain of the orbit sums computed above,

$$
\begin{array}{rcl}
\hat{f}_0 & := & \omega_1^* + \omega_2^* + \omega_3^* + \omega_4^* + \omega_5^* + \omega_6^* + \omega_7^*, \\
\hat{f}_1 & := & \omega_1^*\omega_2^* + \omega_1^*\omega_3^* + \omega_1^*\omega_4^* + \omega_1^*\omega_5^* + \omega_1^*\omega_6^* + \omega_1^*\omega_7^* + \omega_2^*\omega_3^* + \\
 & & \omega_2^*\omega_4^* + \omega_2^*\omega_5^* + \omega_2^*\omega_6^* + \omega_2^*\omega_7^* + \omega_3^*\omega_4^* + \omega_3^*\omega_5^* + \omega_3^*\omega_6^* + \\
 & & \omega_3^*\omega_7^* + \omega_4^*\omega_5^* + \omega_4^*\omega_6^* + \omega_4^*\omega_7^* + \omega_5^*\omega_6^* + \omega_5^*\omega_7^* + \omega_6^*\omega_7^*, \\
\hat{f}_2 & := & \omega_1^*\omega_2^*\omega_3^* + \omega_1^*\omega_2^*\omega_4^* + \omega_1^*\omega_2^*\omega_5^* + \omega_1^*\omega_2^*\omega_7^* + \omega_1^*\omega_3^*\omega_4^* + \omega_1^*\omega_3^*\omega_5^* + \\
 & & \omega_1^*\omega_3^*\omega_6^* + \omega_1^*\omega_4^*\omega_6^* + \omega_1^*\omega_4^*\omega_7^* + \omega_1^*\omega_5^*\omega_6^* + \omega_1^*\omega_5^*\omega_7^* + \omega_1^*\omega_6^*\omega_7^* + \\
 & & \omega_2^*\omega_3^*\omega_5^* + \omega_2^*\omega_3^*\omega_6^* + \omega_2^*\omega_3^*\omega_7^* + \omega_2^*\omega_4^*\omega_5^* + \omega_2^*\omega_4^*\omega_6^* + \omega_2^*\omega_4^*\omega_7^* + \\
 & & \omega_2^*\omega_5^*\omega_6^* + \omega_2^*\omega_6^*\omega_7^* + \omega_3^*\omega_4^*\omega_5^* + \omega_3^*\omega_4^*\omega_6^* + \omega_3^*\omega_4^*\omega_7^* + \omega_3^*\omega_5^*\omega_7^* + \\
 & & \omega_3^*\omega_6^*\omega_7^* + \omega_4^*\omega_5^*\omega_6^* + \omega_4^*\omega_5^*\omega_7^* + \omega_5^*\omega_6^*\omega_7^*, \\
\hat{f}_3 & := & \omega_1^*\omega_2^*\omega_6^* + \omega_1^*\omega_3^*\omega_7^* + \omega_1^*\omega_4^*\omega_5^* + \omega_2^*\omega_3^*\omega_4^* + \\
 & & \omega_2^*\omega_5^*\omega_7^* + \omega_3^*\omega_5^*\omega_6^* + \omega_4^*\omega_6^*\omega_7^*, \\
\hat{f}_4 & := & \omega_1^*\omega_2^*\omega_3^*\omega_5^* + \omega_1^*\omega_2^*\omega_4^*\omega_7^* + \omega_1^*\omega_3^*\omega_4^*\omega_6^* + \omega_1^*\omega_5^*\omega_6^*\omega_7^* + \\
 & & \omega_2^*\omega_3^*\omega_6^*\omega_7^* + \omega_2^*\omega_4^*\omega_5^*\omega_6^* + \omega_3^*\omega_4^*\omega_5^*\omega_7^*,
\end{array}
$$

$$\begin{array}{rcl}
\hat{f}_5 & := & \omega_1^*\omega_2^*\omega_3^*\omega_4^*\omega_5^*\omega_6^* + \omega_1^*\omega_2^*\omega_3^*\omega_4^*\omega_5^*\omega_7^* + \omega_1^*\omega_2^*\omega_3^*\omega_4^*\omega_6^*\omega_7^* + \\
 & & \omega_1^*\omega_2^*\omega_3^*\omega_5^*\omega_6^*\omega_7^* + \omega_1^*\omega_2^*\omega_4^*\omega_5^*\omega_6^*\omega_7^* + \omega_1^*\omega_3^*\omega_4^*\omega_5^*\omega_6^*\omega_7^* + \\
 & & \omega_2^*\omega_3^*\omega_4^*\omega_5^*\omega_6^*\omega_7^*, \\
\hat{f}_6 & := & \omega_1^*\omega_2^*\omega_3^*\omega_4^*\omega_5^*\omega_6^*\omega_7^*.
\end{array}$$

Actually, it turns out that there is no set of primary invariants of $S[W^*]^G$ having a strictly smaller degree product, hence $\hat{\mathcal{F}}$ is optimal in the sense of [5, Ch.3.3.2]. As $\hat{f}_0 \in S[W^*]_1^G$, using the technique described in Remark (3.8), we find an optimal set $\mathcal{F} = \{f_1, , \ldots, f_6\} \subseteq S[W'^*]^G$ of primary invariants, having degrees $\{2, 3, 3, 4, 6, 7\}$.

(4.5) Next we compute secondary invariants of $S[W'^*]^G$. Using the Hilbert series given in Proposition (4.2), we by Proposition (4.3) and Remark (3.3) conclude that there is a minimal set of 18 secondary invariants, having degrees $\{0, 4, 5, 5, 6, 7, 8, 9, 9, 10, 10, 11, 12, 13, 14, 14, 15, 19\}$. To find such a set of secondary invariants, we first compute the homogeneous components $S[W'^*]_d^G$, for $d \leq 7$, using linear algebra techniques, see [5, Ch.3.1], implemented in MAGMA, and then consider products of the homogeneous invariants thus found having appropriate degrees. Thus we successively generate homogeneous elements $\mathcal{G} := \{g_1, g_2, \ldots, g_{18}\} \in S[W'^*]^G$, repeatedly using the method described in Remark (3.9) to ensure that we have $\dim_{\mathbb{F}_2}(\langle \pi(g_j); j \in \{1, \ldots, k\}\rangle_{\mathbb{F}_2}) = k$, for $k \in \{1, \ldots, 18\}$.

To apply the method described in Remark (3.9), we again consider the invariant ring $S[W'^*]^D$, where $D \leq G$ be a 2-Sylow subgroup of G, see the proof of Proposition (4.3). As $S[W'^*]^D$ is Cohen-Macaulay, using linear algebra techniques, implemented in MAGMA, we obtain the finite presentation $S[W'^*]^D \cong \langle F_1, \ldots, F_6, G_1, \ldots, G_3 | R_1, \ldots, R_3\rangle$ as commutative $\mathbb{F}_2$-algebras, where the relations are given as

$$\begin{array}{rcl}
R_1 & := & (F_1 + F_2)^2(F_1F_2F_4 + F_3F_5 + F_4^2 + F_4F_5) + (F_3 + F_4)F_5^2 + \\
 & & (F_1^3 + F_1F_2^2 + F_1F_5 + F_2F_5) \cdot G_1 + (F_1^2F_2 + F_2^3) \cdot G_2 + G_1^2, \\
R_2 & := & (F_1F_2 + F_2^2 + F_3)F_3F_4 + (F_1F_2^2 + F_1F_3 + F_2^3 + F_2F_5) \cdot G_1 + \\
 & & (F_1F_2^2 + F_1F_5 + F_2^3 + F_2F_5) \cdot G_2 + G_1G_2 + G_3, \\
R_3 & := & (F_2^2F_6 + F_3^2F_5) + F_2F_3 \cdot G_2 + G_2^2,
\end{array}$$

where the isomorphism from the finitely presented algebra to $S[W'^*]^D$ is given by $F_i \mapsto f_i'$ and $G_j \mapsto g_j'$, where $\{f_1', \ldots, f_6'\} \subseteq S[W'^*]^D$ and $\{g_1', \ldots, g_3'\} \subseteq S[W'^*]^D$ are as in the proof of Proposition (4.3).

Decomposing the set of primary invariants $\mathcal{F} \subseteq S[W'^*]^G \subseteq S[W'^*]^D$ into the $\mathbb{F}_2$-algebra generators $\{f_1', \ldots, f_6'\} \cup \{g_1', \ldots, g_3'\}$ of $S[W'^*]^D$, again using linear algebra techniques, implemented in MAGMA, finally yields the finite presentation

$$S[W'^*]^D/(\sum_{i=1}^{6} f_i S[W'^*]^D) \cong \langle F_1, \ldots, F_6, G_1, \ldots, G_3 | R_1, , \ldots, R_3, R_1', \ldots, R_6'\rangle$$

as commutative $\mathbb{F}_2$-algebras, where the additional relations are given as

$$\begin{array}{rcl}
R'_1 & := & F_2^2 + F_4 + F_5, \\
R'_2 & := & F_1F_4 + F_2F_5 + G_1 + G_2, \\
R'_3 & := & F_2F_4 + G_1, \\
R'_4 & := & F_1^2(F_1+F_2)^2 + F_1(F_1+F_2)(F_4+F_5) + F_3(F_3+F_4) + F_6 + F_1 \cdot G_1, \\
R'_5 & := & F_1^2(F_3^2 + F_3F_4 + F_6) + F_1F_2(F_2^2F_4F_3F_4 + F_4F_5 + F_6) + \\
 & & F_2^2(F_3F_4 + F_3F_5 + F_4^2) + (F_3+F_4)(F_5^2 + F_6) + F_4^2F_5 + \\
 & & (F_1F_3 + F_1F_5 + F_2^3 + F_2F_4) \cdot G_1 + \\
 & & (F_1F_2^2 + F_1F_3 + F_1F_4 + F_1F_5) \cdot G_2 + G_3, \\
R'_6 & := & F_1F_6(F_3+F_4).
\end{array}$$

Finally, we end up with secondary invariants $\mathcal{G} := \{g_1, \ldots, g_6\} \cup \{g_7, \ldots, g_{18}\}$, where $g_1 = 1$ and $\{g_1, \ldots, g_6\}$ have degrees $\{0, 4, 5, 5, 6, 7\}$, while

$$\begin{array}{rcrr|rcrr|rcrr}
g_7 & := & g_2^2 & (8), & g_{11} & := & g_3g_4 & (10), & g_{15} & := & g_2^2g_5 & (14), \\
g_8 & := & g_2g_3 & (9), & g_{12} & := & g_2g_6 & (11), & g_{16} & := & g_2g_3g_4 & (14), \\
g_9 & := & g_2g_4 & (9), & g_{13} & := & g_2^3 & (12), & g_{17} & := & g_2^2g_6 & (15), \\
g_{10} & := & g_2g_5 & (10), & g_{14} & := & g_2^2g_3 & (13), & g_{18} & := & g_2^3g_6 & (19),
\end{array}$$

where the bracketed numbers indicate the degrees. Hence in particular we conclude that $\{f_1, \ldots, f_6\} \cup \{g_1, \ldots, g_6\} \subseteq S[W'^*]^G$ is a minimal $\mathbb{F}_2$-algebra generating set of $S[W'^*]^G$, and in particular $S[W'^*]^G$ is as an $\mathbb{F}_2$-algebra generated by invariants of degree at most 7.

(4.6) Remark. In conclusion we note the following observations.
a) As W is a transitive permutation module of odd degree in characteristic 2, there is a non-zero G-invariant quadratic form on W. Indeed, this form coincides with the primary invariant $\hat{f}_1 \in S[W^*]^G$ of degree 2. Moreover, we have

$$f_1 = a^*e^* + b^*f^* + c^*d^* + d^*e^* + d^*f^* + e^*f^* + d^{*2} + e^{*2} + f^{*2} \in S[W'^*]^G.$$

Hence this shows that $D_{W'}$ is an embedding $D_{W'} \colon G \to SO_6^+(\mathbb{F}_2)$, where $SO_6^+(\mathbb{F}_2)$ denotes the special orthogonal group of degree 6 over $\mathbb{F}_2$ of maximal Witt index type, see [3, p.22].

b) We have $\{0\} \to (W'/W'')^* \to W'^* \to W''^* \to \{0\}$, see Section (2.3). Note that this extension does not split: Assume to the contrary it splits. Then we also have $W' \cong W'' \oplus W'/W''$, and hence $(\mathbb{F}_2)_H^G \cong W \cong W'' \oplus W'/W'' \oplus \mathbb{F}_2$ is semisimple, and thus $\dim_{\mathbb{F}_2}(\mathrm{End}_G((\mathbb{F}_2)_H^G)) = 3$. By the proof of Proposition (4.2) we have $\dim_{\mathbb{Q}_2}(\mathrm{End}_G((\mathbb{Q}_2)_H^G)) = 2$, a contradiction to [1, Thm.3.11.3].

Still we are tempted to apply the technique described at the beginning of Remark (3.8), yielding an embedding $S[W'^*]^G/((W'/W'')^*S[W'^*])^G \to S[W''^*]^G$. The question arises whether this map is still surjective. While the authors do not see a structural reason why this should be the case, from the primary invariants $\{f_4, f_5, f_6\} \subseteq S[W'^*]^G$ of degrees $\{4, 6, 7\}$ we obtain $\{c_0, c_1, c_2\} \subseteq S[W''^*]^G$,

given as

$$\begin{array}{rcl} c_2 & := & a^{*4}+b^{*4}+c^{*4}+a^{*2}b^{*2}+a^{*2}c^{*2}+b^{*2}c^{*2}+ \\ & & a^{*2}b^*c^*+a^*b^{*2}c^*+a^*b^*c^{*2}, \\ c_1 & := & a^{*4}b^{*2}+a^{*2}b^{*4}+a^{*4}c^{*2}+a^{*2}c^{*4}+b^{*4}c^{*2}+b^{*2}c^{*4}+ \\ & & a^{*4}b^*c^*+a^*b^{*4}c^*+a^*b^*c^{*4}+a^{*2}b^{*2}c^{*2}, \\ c_0 & := & a^{*4}b^{*2}c^*+a^{*4}b^*c^{*2}+a^{*2}b^{*4}c^*+a^*b^{*4}c^{*2}+a^{*2}b^*c^{*4}+a^*b^{*2}c^{*4}. \end{array}$$

It turns out that these are the **Dickson invariants** of $S[W''^*]^G$, see [2, Ch.8.1]. By Dickson's Theorem, see [2, Thm.8.1.1], the set $\{c_0, c_1, c_2\} \subseteq S[W''^*]^G$ is algebraically independent, and we have $S[W''^*]^G = \mathbb{F}_2[c_0, c_1, c_2]$. Hence the above map $S[W'^*]^G/((W'/W'')^* S[W'^*])^G \to S[W''^*]^G$ indeed is surjective.

c) Using the technique described in Remark (3.8), we may also find an optimal set of primary invariants of the invariant ring $S[\widetilde{W'^*}]^G$, which by the Hochster-Eagon Theorem, see [2, Thm.4.3.6] or Proposition (3.7), is Cohen-Macaulay. These optimal primary invariants turn out to have degrees $\{2, 3, 3, 4, 4, 7\}$. Indeed, the Hilbert series $H_{S[\widetilde{W'^*}]^G}(t) = H_{S[W'^*]^G}(t) \in \mathbb{Q}(t)$, see the proof of Proposition (4.2), can be rewritten as

$$H_{S[\widetilde{W'^*}]^G}(t) = \frac{1 + 2t^5 + 2t^6 + t^7 + t^{10} + 2t^{11} + 2t^{12} + t^{17}}{(1-t^2)\cdot(1-t^3)^2\cdot(1-t^4)^2\cdot(1-t^7)}.$$

Since the optimal set $\mathcal{F}$ of primary invariants has degrees $\{2, 3, 3, 4, 6, 7\}$, there is no set of primary invariants of $S[W'^*]^G$ having degrees $\{2, 3, 3, 4, 4, 7\}$. This shows, although $S[\widetilde{W'^*}]^G$ and $S[W'^*]^G$ do have the same Hilbert series, that their ring structures are different. Still, as the underlying modules W'^* and $\widetilde{W'^*}$ are closely related, the corresponding invariant rings should be closely related as well. But how this relationship might look like, for the time being remains mysterious to the authors.

References

[1] D. Benson: Representations and cohomology I, Cambridge Studies in Advanced Mathematics 30, Cambridge Univ. Press, 1991.

[2] D. Benson: Polynomial invariants of finite groups, London Mathematical Society Lecture Note Series 90, Cambridge Univ. Press, 1993.

[3] J. Conway, R. Curtis, S. Norton, R. Parker, R. Wilson: Atlas of finite groups, maximal subgroups and ordinary characters for simple groups, Oxford Univ. Press, 1985.

[4] The Computational Algebra Group: MAGMA-V2.10 — The Magma Computational Algebra System, School of Mathematics and Statistics, University of Sydney, 2003, `http://magma.maths.usyd.edu.au/magma/`.

[5] H. Derksen, G. Kemper: Computational invariant theory, Encyclopedia of Mathematical Sciences 130, Springer, 2000.

[6] J. Dixmier: On the projective invariants of quartic plane curves, Adv. in Math. 64, 1987, 279–304.

[7] N. Elkies: The Klein quartic in number theory, The eightfold way, 51–101, Math. Sci. Res. Inst. Publ. 35, Cambridge Univ. Press, 1999.

[8] The GAP Group: GAP-4.3 — Groups, Algorithms and Programming, Aachen, St. Andrews, 2003, `http://www-gap.dcs.st-and.ac.uk/gap/`.

[9] C. Jansen, K. Lux, R. Parker, R. Wilson: An atlas of Brauer characters, London Mathematical Society Monographs, New Series 11, Oxford Univ. Press, 1995.

[10] E. Nart, C. Ritzenthaler: Non-hyperelliptic curves of genus three over finite fields of characteristic two, 2003, `http://front.math.ucdavis.edu/math.NT/0312366`.

[11] L. Smith: Polynomial invariants of finite groups, Research Notes in Mathematics 6, Peters, 1995.

J. M.:
Lehrstuhl D für Mathematik, RWTH Aachen,
Templergraben 64, D-52062 Aachen, Germany;
`Juergen.Mueller@math.rwth-aachen.de`.

Institut für Experimentelle Mathematik (IEM),
Universität Duisburg-Essen,
Ellernstrasse 29, D-45326 Essen, Germany.

C. R.:
Institut für Experimentelle Mathematik (IEM),
Universität Duisburg-Essen,
Ellernstrasse 29, D-45326 Essen, Germany.
`ritzenth@math.jussieu.fr`.